

# HARDENING DE SERVIDORES LINUX

## • Segurança Física (Acesso Local)

### 1) Senha no Grub (Ubuntu) (CRIE SNAPSHOTS DA VM ANTES DE INICIAR):

- a) `# grub-mkpasswd-pbkdf2 >grubpass.txt` - redireciona para um arquivo de texto
- b) `# vim grubpass.txt` – editar o arquivo de texto com o hash da senha do grub como abaixo:

`cat<< EOF`

`set superusers="admin"`

Tudo numa linha só

```
password_pbkdf2 admin
grub.pbkdf2.sha512.10000.2E76F00F221375A635334DEE22E9EF48A3C752EDCFA01221789FDFFE
34251C23C1EF11E39CF13EB525D4E99008598CE81035EF0AA67C8B4F0569B0C3BE5A20F1.0A43B
4FC74BF2EEE479E3CE0697B933BC7249894029523CEF2D01605480FA869CAA9B44BFCBAB431633
8EF6DDA9F8D4E30E996FB14E2ED0B42B05F5435778A73
```

`EOF`

- c) `# cat grubpass.txt >> /etc/grub.d/00_header` – redirecionar para o arquivo do grub lido no boot. CUIDADO EM USAR >> E NÃO >
- d) `# cat /etc/grub.d/00_header` – verifique se está ok com as informações no final do arquivo

```
cat<<EOF
set superusers="professor"

password_pbkdf2 professor grub.pbkdf2.sha512.10000.3643181084D9B01EEC1EB36A9CE6098D6F7E0FFF1EEEA03D0
1453D8ADB01CE1A9C2E5B80439831BD7DAE81663A373D8B70FE70B621C904EB0AE8E72172C87049.0D8ADA92CE966590B56D
9EB98EDEE41AC4BD2D55FD5D9A7E6DB6264BDF8488B9C1F9AB9E895D718F5F9013F7F259366F6A8CE6331C0066114FDA219C
DB6BD784
EOF
```

- e) `# update-grub2` – atualiza as informações adicionadas ao grub
- f) `# reboot`

## 2) Remover Módulos (drivers de dispositivos) sem uso

a) *Encontre módulos pelo nome*

```
# find /lib/modules -iname *firewire*
```

b) *Encontre módulos pela versão do kernel*

```
# find /lib/modules/$(uname -r) -print
```

c) *Verificar os módulos em blacklist*

```
# modprobe --showconfig | egrep "^(blacklist|install)"
```

d) *Informações de um modulo*

```
# modinfo psmouse
```

e) *Remover um módulo do sistema, carregado na memória*

```
# modprobe -r psmouse
```

f) *Colocar um module em blacklist (desativar)*

```
# vim /etc/modprobe.d/blacklist.conf
```

```
blacklist psmouse
```

## 3) Dispositivos USB (pendrive, hds,etc) desativar o driver de storage (desativa tudo!)

```
# lsmod | grep usb_storage
```

- Método 1

```
# echo 'install usb-storage /bin/true' > /etc/modprobe.d/fake_usb.conf
```

- Método 2

```
# mv /lib/modules/$(uname -r)/kernel/drivers/usb/storage/usb-storage.ko /home/centlinux
```

- Método 3

```
# echo 'blacklist usb-storage' >> /etc/modprobe.d/blacklist.conf
```

- 4) – USBGUARD – Crie políticas (*block – reject – allow*) para USB Storage (Pendrive / HD Externo)  
Pode ser utilizado em qualquer Linux troque o dnf pelo apt ou zypper

- a) *# dnf install usbguard usbutils udisks2 – instale os pacotes*
- b) *# usbguard generate-policy > /etc/usbguard/rules.conf – gere a política padrão*
- c) *# systemctl enable --now usbguard – ative o serviço*
- d) *# systemctl status usbguard – verifique se está rodando*
- e) *# lsusb – listagem dispositivos no barramento usb*
- f) *# usbguard list-devices – liste os dispositivos (número, serial e hash)*
- g) *# usbguard block-device 6 – regra que bloqueia o dispositivo 6*

- 5) Auto Logout após tempo. Permanente e para todos e temporário para o usuário logado

- a) *Forma permanente*  
*# vim /etc/profile*

**TMOUT=600**

- b) *Imediato e Temporário*

*# export TMOUT=300*

## ● Instalação - Partições e Sistemas de Arquivos

- 1) Efetuar instalações mínimas ou usar versões mínimas das distribuições e adicionar somente os serviços e pacotes necessários.

Ubuntu Server, Rocky Linux Minimal, OpenSuse (Instalação mínima), etc.

- 2) Criar as partições separadas no servidor e criptografe-as (UC13)

/(root)  
/boot  
/home  
/tmp  
/var

- 3) NODEV, NOSUID e NOEXEC em pontos de montagem limitando execução de softwares em locais específicos.

a) Editando o fstab e configurando

# vi /etc/fstab

**/tmp            /var/tmp            none rw,noexec,nosuid,nodev,bind 0            0**

# mount -o rw,noexec,nosuid,nodev,bind /tmp/ /var/tmp/

# mount -o remount,noexec,nosuid,nodev /tmp

# mount -o remount,noexec,nosuid,nodev /dev/shm

# mount | egrep --color -w '^({tmpfs|/tmp})|/tmp'

#### 4) Verificar diretórios (rw) sem Stickybit

# df --local -P | awk '{if (NR!=1) print \$6}' | xargs -l '{}' find '{}' -xdev -type d \( -perm -0002 -a ! -perm -1000 \) 2>/dev/null

#### 5) Verificar e ajustar perms /boot ( grub ou grub2)

# stat /boot/grub2/grub.cfg

Access: (0400/-r-----) Uid: ( 0/ root) Gid: ( 0/ root)

# chown root:root /boot/grub2/grub.cfg

# chmod og-a /boot/grub2/grub.cfg

# chmod 0400 /boot/grub2/grub.cfg

## • Software e S.O.

### 1) Verifique os repositórios se há repositórios suspeitos

**# dnf repolist - sistemas baseados em red hat (rocky Linux, alma Linux, etc.)**

**# apt-cache policy – sistemas baseados em debian (ubuntu)**

**# zypper repos – (Suse OpenSuse Linux)**

## 2) Checar integridade dos pacotes (pacotes adulterados)

**# apt-key list**

**# zypper repos**

## 3) Restringir informações do core dump (erros) deve ser 0

**# sysctl fs.suid\_dumpable**

fs.suid\_dumpable = 2

**# sysctl -w fs.suid\_dumpable=0**

fs.suid\_dumpable = 0

## 4) Verificar habilitar ASLR (Address space layout randomization)

**# sysctl kernel.randomize\_va\_space**

kernel.randomize\_va\_space = 2

**# sysctl -w kernel.randomize\_va\_space=2**

# • Updates e Hotfix

## 1) Verifique repos

## 2) Verifique os updates e upgrades disponíveis

**# dnf check-update – *checar no red hat (rocky linux)***

**# apt-get -s upgrade – *checar no Debain/Ubuntu***

**# apt list --upgradable - *checar no Ubuntu***

**# zypper list-updates – *checar no Suse***

## 3) Realizar updates e upgrades

**# apt-get upgrade – *Atualizar versões de pacotes***

**# apt-get dist-upgrade – *Atualizar toda a distribuição***

**# dnf update - *Atualizar versões de pacotes***

#### 4) Automatic Updates

##### Ubuntu Server:

```
# apt install unattended-upgrades
```

```
# apt install apticron
```

Editar /etc/apticron/apticron.conf:

```
# Colocar o email para onde será entregue os relatórios de atualizações
```

```
# Exemplo: suporte@empresa.com.br
```

```
EMAIL=root
```

```
# apticron
```

```
# less /var/mail/root
```

##### Red Hat (Rocky):

```
# dnf install dnf-automatic
```

```
# vim /etc/dnf/automatic.conf
```

```
apply_updates = yes
```

```
emit_via = motd
```

```
upgrade_type = security
```

```
email_from = root@example.com
```

```
email_to = root
```

```
# systemctl enable --now dnf-automatic.timer
```

```
# vim /etc/systemd/system/timers.target.wants/dnf-automatic.timer
```

```
OnCalendar=*-*-* 01:00
```

```
# systemctl daemon-reload
```

```
# systemctl list-timers
```

## ● Serviços

#### 1) Verificar quais serviços estão ativos

```
# systemctl -t service --state=active
```

***# netstat -lp -A inet***

***Ou***

***# ss -ltn -A inet***

***# netstat -ltn -A inet***

Use **ss** no lugar do **netstat** se necessário

## 2) Instalar configurar serviço de Hora

***# dnf install ntp (ou chrony)***

***# apt-get install ntp (ou chrony)***

***# zypper install ntp (ou chrony)***

/etc/ntp.conf ou /etc/chrony.conf

***server <remote-server>***

***OPTIONS="-u ntp:ntp"***

***NTPD\_OPTIONS="-u ntp:ntp"***

***RUNASUSER=ntp***

## 3) Verificar se o X11 não está instalado

***# rpm -qa xorg-x11\****

***# dpkg -l xserver-xorg\****

***# dnf remove xorg-x11\****

***# apt-get remove xserver-xorg\****

***# zypper remove xorg-x11\****

## 4) Verificar os serviços diversos se habilitados

***# systemctl is-enabled avahi-daemon***

***# systemctl is-enabled cups***

***# systemctl is-enabled dhcpcd***

***# systemctl is-enabled slapd***

***# systemctl disable slapd***

***# systemctl is-enabled nfs***

***# systemctl is-enabled rpcbind***

```
# systemctl is-enabled named
# systemctl is-enabled vsftpd
# systemctl is-enabled httpd (ou apache2)
# systemctl is-enabled dovecot
# systemctl is-enabled smb (smbd)
# systemctl is-enabled nmb (nmbd)
# systemctl is-enabled squid
# systemctl is-enabled snmpd
# systemctl is-enabled rsyncd
# systemctl is-enabled yperv
```

5) Verificar os clientes diversos se instalados

```
# rpm -q ypbind (red hat) – cliente do NIS
# dpkg -s ypbind (debian) – ""
# rpm -q rsh - cliente do remote shell
# dpkg -s rsh – ""
# rpm -q talk - client de chat no shell
# dpkg -s talk – ""
# rpm -q telnet – client telnet
# dpkg -s telnet – ""
# rpm -q openldap-clients - cliente openldap
# dpkg -s openldap-clients – ""
```

## • Rede e Protocolos

1) Verificar se há encaminhamentos, redirecionamentos habilitados

```
# sysctl net.ipv4.ip_forward
net.ipv4.ip_forward = 0
```

```
# grep "net\.ipv4\.ip_forward" /etc/sysctl.conf
/etc/sysctl.d/* net.ipv4.ip_forward = 0
```

```
# sysctl net.ipv6.conf.all.forwarding
net.ipv6.conf.all.forwarding = 0
```

```
# grep "net\.ipv6\.conf\.all\.forwarding" /etc/sysctl.conf /etc/sysctl.d/*
net.ipv6.conf.all.forwarding = 0
# sysctl net.ipv4.conf.all.send_redirects
net.ipv4.conf.all.send_redirects = 0
```



```
# sysctl net.ipv4.conf.default.send_redirects
```

```
net.ipv4.conf.default.send_redirects = 0
```

```
# grep "net\.ipv4\.conf\.all\.send_redirects" /etc/sysctl.conf /etc/sysctl.d/*
```

```
net.ipv4.conf.all.send_redirects = 0
```

```
# grep "net\.ipv4\.conf\.default\.send_redirects" /etc/sysctl.conf /etc/sysctl.d/*
```

```
net.ipv4.conf.default.send_redirects= 0
```

## 2) Verificar cookies SYN (evitar syn flood)

```
# sysctl net.ipv4.tcp_syncookies
```

```
net.ipv4.tcp_syncookies = 1
```

```
# grep "net\.ipv4\.tcp_syncookies" /etc/sysctl.conf /etc/sysctl.d/*
```

```
net.ipv4.tcp_syncookies = 1
```

- desabilitar ipv6

```
net.ipv6.conf.all.disable_ipv6 = 1
```

```
net.ipv6.conf.default.disable_ipv6 = 1
```

```
net.ipv6.conf.lo.disable_ipv6 = 1
```

## 3) Realizar alterações

```
# sysctl -w net.ipv4.tcp_syncookies=1
```

## 4) Portas abertas protocolos e processos

```
# ps -ef
```

```
# netstat -antp | grep ESTABLISHED
```

```
# netstat -antp | grep LISTEN
```

```
# ss -antp | grep ESTABLISHED
```

```
# ss -antp | grep LISTEN
```

# ● Contas

## 1) Limitar recursos

```
#ulimit -u
```

```
#ulimit -a
```

```
#ulimit -S -u 5000
```

```
#pgrep -wcu $USER
```

## ● Senhas

### 1) Gerar senhas fortes

```
# pwmake 128 – Red Hat distros
```

```
# apt install -y apg – Ubuntu
```

```
# apg
```

### 2) Complexidade da senhas. Tentativas 3 vezes

```
# apt install libpam-pwquality – Ubuntu
```

```
# vim /etc/pam.d/common-password – Ubuntu
```

```
# vim /etc/pam.d/passwd - Red hat
```

```
password    required    pam_pwquality.so    retry=3
```

### 3) Política de senhas:

```
# vim /etc/security/pwquality.conf
```

```
minlen = 8
```

```
minclass = 4
```

```
maxsequence = 3
```

```
maxrepeat = 3
```

## ● Permissões

### 1) Buscar e desabilitar arquivos SUID e SGID

```
# find / -path /proc -prune -o -type f \( -perm -4000 -o -perm -2000 \) -exec ls -l {} \;
```

Ou

```
# find / -perm -4000 -print – verifica SUID nos arquivos
```

```
# find / -perm -2000 -print - verifica SGID nos arquivos
```

```
# chmod u-s /path/to/binary_file
```

```
# chmod g-s /path/to/binary_file
```

2) Arquivos e diretórios sem donos

```
# find / -nouser -o -nogroup -exec ls -l {} \;
```

3) Lista de arquivos graváveis

```
# find / -path /proc -prune -o -perm -2 ! -type l -ls
```

## ● Logs

1) Logs a verificar e monitorar:

```
# /var/log/auth.log – autenticação/login Ubuntu
```

```
# /var/log/secure - autenticação/login Red Hat
```

```
# /var/log/boot.log
```

```
# /var/log/dmesg
```

```
# /var/log/kern.log
```

```
# /var/log/faillog
```

```
# /var/log/cron
```

```
# /var/log/dnf.log
```

```
# /var/log/maillog ou /var/log/mail.log
```

```
# /var/log/httpd/
```

```
# /var/log/mysqld.log or /var/log/mysql.log
```

## ● Auditoria (Manual)

1) Arquivos alterados nos últimos 5 dias

```
# find / -mtime -5 -o -ctime -5 2>/dev/null
```

2) Jobs agendados no servidor

```
# /var/spool/cron/crontabs/
```

```
# /etc/crontab (crontab -e)
```

```
# /etc/cron.d/
```

```
# /etc/cron.hourly/
```

```
# /etc/cron.daily/
```

```
# /etc/cron.weekly/
```

*# /etc/cron.monthly/*

*# crontab -l*

*# crontab -l -u usuario*

## ● Firewall (Ubuntu Server – Red Hat )

### 1) Firewall (Ubuntu Server) ufw:

HABILITAR:

***sudo ufw enable***

DESABILITAR:

***sudo ufw disable***

STATUS:

***sudo ufw status***

STATUS DETALHADO:

***sudo ufw status verbose***

REGRAS PARA PERMITIR TRAFEGO:

***sudo ufw allow <port>/<optional: protocol>***

***sudo ufw allow 53***

***sudo ufw allow 53/tcp***

***sudo ufw allow 53/udp***

REGRAS PARA NEGAR TRAFEGO:

***sudo ufw deny <port>/<optional: protocol>***

***sudo ufw deny 53***

***sudo ufw deny 53/tcp***

***sudo ufw deny 53/udp***

DELETAR REGRAS:

***ufw deny 80/tcp***

***ufw delete deny 80/tcp***

LOG DO FW:

***sudo ufw logging on***

***sudo ufw logging off***

PERMITIR TRAFEGO DE IP:

***sudo ufw allow from 207.46.232.182***

PERMITIR TRAFEGO DE SUBNET:

***sudo ufw allow from 192.168.1.0/24***

PERMITIR TRAFEGO DE IP E PORTA

***sudo ufw allow from 192.168.0.4 to any port 22***

PERMITIR TRAFEGO DE IP PORTA E PROTOCOLO

***sudo ufw allow from PC01.SENAC.SMP to any port 22 proto tcp***

PING (ICMP) BLOQUEAR:

Editar /etc/ufw/before.rules comentar as seguintes linhas ou mudar para DROP:

***# ok icmp codes***

***-A ufw-before-input -p icmp --icmp-type destination-unreachable -j ACCEPT***

***-A ufw-before-input -p icmp --icmp-type source-quench -j ACCEPT***

***-A ufw-before-input -p icmp --icmp-type time-exceeded -j ACCEPT***

***-A ufw-before-input -p icmp --icmp-type parameter-problem -j ACCEPT***

***-A ufw-before-input -p icmp --icmp-type echo-request -j ACCEPT***

ALTERAR REGRAS NUMERADAS

LISTAR

***ufw status numbered***

DELETAR REGRA NUMERADA

***ufw delete 1***

INSERIR REGRA NUMERADA:

***ufw insert 1 allow from <ip address>***

- EXEMPLO BLOQUEAR ORIGEM E DESTINO:

***ufw deny from 192.168.0.1 to any port 22***

***ufw deny from 192.168.0.7 to any port 22***

***ufw allow from 192.168.0.0/24 to any port 22 proto tcp***

## 2) Firewall (Red Hat / Centos Server) firewalld:

HABILITAR E INICIAR:

***# systemctl start firewalld***  
***# systemctl enable firewalld***

DESABILITAR E PARAR:

***# systemctl stop firewalld***  
***# systemctl disable firewalld***

STATUS:

***# firewall-cmd --state***

RELOAD CONFIGS:

***# firewall-cmd --reload***

ARQUIVOS DE CONFIGS:

/etc/firewalld/

CONFIGURAÇÃO PERMANENTE E RELOAD:

***# firewall-cmd --zone=public --add-service=http --permanent***  
***# firewall-cmd --zone=public --add-service=http***

***# firewall-cmd --zone=public --add-service=http --permanent***  
***# firewall-cmd --reload***

LISTAR ZONAS:

***# firewall-cmd --list-all-zones***

ZONA DEFAULT:

***# firewall-cmd --get-default-zone***

DEFINIR ZONA DEFAULT:

***# firewall-cmd --set-default-zone=internal***

ZONA ATIVAS POR INTERFACE:

***# firewall-cmd --get-active-zones***

CONFIGURAÇÕES DE UMA ZONA ESPECIFICA:

***# firewall-cmd --zone=public --list-all***

SERVIÇOS:

***# firewall-cmd --get-services***

SERVIÇOS (/etc/firewalld/services) ADD E REMOVE :

```
# firewall-cmd --zone=public --add-port=12345/tcp --permanent
# firewall-cmd --zone=public --remove-port=12345/tcp --permanent
```

PORTAS PERMITIR NEGAR:

```
# firewall-cmd --zone=public --add-port=12345/tcp --permanent
# firewall-cmd --zone=public --remove-port=12345/tcp --permanent
```

PORT FORWARD (ENCAMINHAMENTO DE PORTA 80 PARA 12345):

```
# firewall-cmd --zone="public" --add-forward-port=port=80:proto=tcp:toport=12345
```

ATIVAR MASQUERADE EM UMA ZONA (PUBLIC):

```
# firewall-cmd --zone=public --add-masquerade
```

ENCAMINHAMENTO PORTA LOCAL 80 PARA PORTA REMOTA 8080:

```
# firewall-cmd --zone="public" --add-forward-
port=port=80:proto=tcp:toport=8080:toaddr=198.51.100.0
```

REMOVER REGRAS:

```
# firewall-cmd --zone=public --remove-masquerade
```

EXEMPLO DE REGRAS PARA DEFINIR UMA ZONA DMZ NA ETH0:

```
# firewall-cmd --set-default-zone=dmz
# firewall-cmd --zone=dmz --add-interface=eth0
# firewall-cmd --reload
# firewall-cmd --zone=dmz --list-all
```

---

## • Anti-Malware – Rootkit – Brute Force – Auditoria automatizada

### 1. AUDITD – Auditoria de Segurança

```
# dnf install auditd
```

```
# apt install auditd  
# systemctl enable auditd  
# systemctl start auditd  
# auditctl -l  
# auditctl -w /etc/passwd -p wa -k user-modify  
# useradd testuser  
# cat /var/log/audit/audit.log | grep user-modify
```

Configuração persistente edite o arquivo:

```
/etc/audit/rules.d/audit.rules  
-w /etc/passwd -p wa -k user-modify  
# ausearch -i -k user-modify  
# aureport -x
```

## 2. **CHKROOTKIT – Scan de rootkit**

```
# chkrootkit
```

## 3. **RKHUNTER – Scan de rootkit**

```
# apt install rkhunter  
# rkhunter --check  
# rkhunter --update  
# rkhunter --propupd
```

## 4. **LYNIS :Auditoria de segurança, teste de conformidade, teste de intrusão, detecção de vulnerabilidade e hardening do sistema**

```
# lynis  
# lynis show  
# lynis show version  
# lynis show tests
```



***# lynis audit system***

**Converter o relatório .dat em html:**

*# lynis audit system | ansi2html -l > report.html*

## 5. ClamAv – Antivirus Open Source

***# dnf install clamav***

***# apt-get install clamav clamav-daemon***

***# freshclam***

***# clamscan -r /home/user***

***# clamscan -r /***

***# clamscan --infected --remove --recursive /home/user***

Se quiser testar baixe um virus de teste:

***#wget -c <https://secure.eicar.org/eicar.com>***

## 6. OPENSCAP – Scanner de Vulnerabilidades Linux

***# dnf install openscap-scanner bzip2***

***# wget -O - https://www.redhat.com/security/data/oval/v2/RHEL8/rhel-8.oval.xml.bz2 | bzip2 --decompress > rhel-8.oval.xml***

***# oscap oval eval --report vulnerability.html rhel-8.oval.xml***

**UBUNTU:**

***# apt -y install libopenscap8 bzip2***

***# wget https://security-metadata.canonical.com/oval/com.ubuntu.\${lsb\_release -cs}.usn.oval.xml.bz2***

***# bzip2 -d com.ubuntu.jammy.usn.oval.xml.bz2***

***# oscap oval eval --report oval-jammy.html com.ubuntu.jammy.usn.oval.xml***

## 7. FAIL2BAN – Defesa contra bruteforce e outros

```
# apt install fail2ban
```

```
# dnf install fail2ban
```

Criar ou editar arquivo jail.local (/etc/jail.local):

```
[ssh]
```

```
enabled = true
```

```
filter = sshd
```

```
action = iptables[name=ssh, port="ssh", protocol=tcp]
```

```
logpath = /var/log/fail2ban.log
```

```
maxretry = 3
```

```
bantime = 10m
```

```
ignoreip = 127.0 ::1
```

```
# systemctl start fail2ban
```

Ver status dos jails do serviço:

```
# fail2ban-client status
```

```
# fail2ban-client status ssh
```

Liste as regras de firewall antes e depois de usar o brute force para teste:

```
# iptables -L
```

Teste fazendo um ataque brute force de outra máquina :

```
# ncrack -vv --user root -P password.txt 192.168.1.208:22
```

Para ver se uma porta TCP responde, antes e depois do fail2ban bloquear:

```
# hping3 -S 72.14.207.99 -p 80 -c 1
```

Desbloquear um host sem esperar o tempo de bloqueio:

```
# fail2ban-client unban 192.168.1.208
```

Ver os logs das tentativas de logon/login (brute force)

```
# tail /var/log/fail2ban.log
```

## **8. AIDE (Tripwire HIDS) detectar rootkits e malwares**

```
# dnf install aide
```

```
# dnf install aide
```

```
# apt-get install aide
```

```
# zypper install aide
```

```
# aide --init
```

```
# mv /var/lib/aide/aide.db.new.gz /var/lib/aide/aide.db.gz
```

```
# aide --check
```

Agendar checagem:

```
# crontab -e
```

```
05 4 * * * root /usr/sbin/aide --check
```

```
# aide --update
```